STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G4: Mainframe Security

1. INTRODUCTION:

Security controls for mainframe information systems using the International Business Machines (IBM) OS/390 or z/OS operating system have been developed by IBM and documented in IBM and other source references. Consistent application of these controls ensures operating system integrity is maintained and results in a substantial reduction in vulnerability exposure.

2. OBJECTIVE:

Establish a baseline configuration for mainframe equipment owned and/or operated by the State of Alabama.

3. SCOPE:

These recommendations apply to mainframe systems utilizing z/OS or OS/390.

4. GUIDELINES:

4.1 GENERAL SECURITY REQUIREMENTS

Mainframe systems shall comply with all applicable State IT Policies and Standards including but not limited to those pertaining to physical security, password usage, system access, remote access, risk and vulnerability management, backup and recovery, and information protection.

Mainframe systems security controls shall be fully documented in system security plans. Plans shall be reviewed in accordance with applicable requirements.

4.2 MAINFRAME SYSTEM CONFIGURATION GUIDELINES

The Defense Information Systems Agency (DISA) OS/390 & z/OS Security Technical Implementation Guide (STIG) defines a secure computing baseline for mainframe systems running the z/OS and OS/390 operating systems. STIG recommendations also include configuration settings for MQ Series/WebSphere MQ, Resource Access Control Facility (RACF), and other mainframe applications.

The OS/390 STIG is available for download from http://iase.disa.mil/stigs/stig/index.html.

Mainframe support personnel should use the OS/390 STIG requirements/recommendations as a reference and implement the applicable security controls. The implemented controls should be fully documented in local guidelines or operational procedures and shall be documented in system security plans (as described in 4.1 above).

4.3 EXCEPTIONS

RACF policies and procedures have been established and documented by State RACF Administration; ISD Planning, Standards and Compliance Office. These policies override any similar guidance in the DISA OS/390 STIG. RACF Administrators shall be provided training on these policies, and copies of these policies shall be provided to administrators upon completion of training.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-02: System Security
http://isd.alabama.gov/policy/Policy_660-02_System_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/20/2008	